UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/026,813	12/27/2001	Hiroo Nakano	217781US2S	1908

22850 7590 11/07/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 11/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/026,813	NAKANO, HIROO	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4 and 11-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4 and 11-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12-27-01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-4 and 11-14 are pending in this office action, claims 5-10 and 15-20 are newly canceled.

2. Applicant's arguments, filed August 12, 2005, have been full considered but they are not persuasive.

Claim Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-4 and 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ugon et al. (U.S. Patent No. 6,839,849) in view of Feyt et al. (U.S. Patent No. 6,698,662).

Regarding claims 1, 3, 11 and 13: Ugon discloses a data processing apparatus/memory card comprising:

- An operation processing unit (FIG.1 item 1) having at least a read cycle period when said operation processing unit reads data from a device (Col 5, Lines 65-

67), and a write cycle period when said operation processing unit writes data in the device (Col 6, Lines 2-5);

- A memory which performs data transmission/reception between said operation processing unit and said memory;(Col 5, Lines 62-65 and Col 6, Lines 12-17)
- A data bus connected to said operation processing unit and said memory;(Col 5, Lines 3-10) and
- A pseudo-data generating circuit connected to said data bus,(Col 11, Lines 14-18) said pseudo-data generating circuit which generates pseudo-data and outputs the pseudo-data to said memory to cause instruction to randomly execute (Col 11, lines 22-25)

Ugon doesn't explicitly disclose the pseudo-data generating circuit outputs the pseudo-data to said data bus in a time interval between the read cycle period and the write cycle period, between the write cycle period and the read cycle period, between two read cycle periods, or between two write cycle periods.

However Feyt et al. discloses a method for hiding operation performed by microprocessor card where he teaches presenting a random data items on the data bus during cryptographic calculation like read and write operations (Col 2, Lines 36-42 and Col 3, Lines 34-52).

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the Ugon system with the teaching of Feyt to output pseudo-data on the data bus between read and write cycles. One would be motivated to

do so in order to mask the power consumption by the memory during the reading or writing of secret data to prevent an attacker from deducing the data by correlation or differential power analysis attacks. (Col 1, lines 36-46)

Regarding claims 2, 4, 12 and 14: Ugon as modified by Feyt et al. discloses the data processing apparatus according to claim 1, wherein said pseudo-data generating circuit generates random number data as the pseudo-data. (see Col 11, Lines 14-18 and Col 12, lines 34-37 of Ugon)

Response to Arguments

5. Applicant argues the combination of references does not teach a single data bus connecting the memory, the operation processing unit, and the pseudo-data generating circuit. Applicant also argues the random number of Ugon is not output to a data bus and there is no structure or functionality corresponding to the pseudo-data generating circuit.

Regarding applicant's arguments, the examiner disagrees with applicant. First, examiner would like to point out that the independent claim does not say anything about the purpose of the pseudo-data generating circuit, as argued by applicant on page 8, first paragraph. Referring to that section of the applicant's arguments, applicant says the independent claim contains "thereby preventing secret data from leaking by applying the pseudo-data to the data but connected to the memory and the operation processing

unit." This limitation is not in the claims and therefore carries no weight. Further, column 5, lines 19-21 says that "the integrated circuit according to the invention also comprises an input/output circuit (14) connected to the only bus..." This sentence is for one embodiment of the invention, mainly an embodiment where there is only one bus. Also, figure 3 shows another embodiment, where there is only one data bus (3) to be shared between the processors and the memory. In this embodiment, the structure required by the instant application is achieved. Mainly, a operation processing unit (fig. 3, ref. num 1) is connected to a memory (fig. 3, RAM/ROM) and a data bus (fig. 3, ref. num 3) with a pseudo-data generating circuit connected to the data bus (col. 11, lines 13-25). This structure shows the secondary processor generating and outputting pseudo-data to the data bus of the primary processor (see page 8, second paragraph of applicant's arguments) because the primary processor and secondary processor are on the same bus.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100